МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
Математического обеспечения ЭВМ

Абрамов Г.В.

21.06.2021г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.06 Безопасность мобильных приложений

1. Код и наименование направления подготовки/специальности:

02.04.02 Фундаментальная информатика и информационные технологии

2. Профиль подготовки/специализация:

Программирование для мобильных устройств

3. Квалификация (степень) выпускника: магистр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: МО ЭВМ

6. Составители программы: Тютин Антон Павлович,
преподаватель

7. Рекомендована: НМС факультета ПММ, протокол № 10 от 15.06.2021

_____

отметки о продлении вносятся вручную)

_____

8. Учебный год: 2019/2020 Семестр(ы): 3

9.Цели и задачи учебной дисциплины: Цели дисциплины – получение фундаментальных знаний в области теоретических основ информационной безопасности; формирование у обучающихся системно-информационного взгляда на подходы для обеспечения безопасности мобильных приложений.

Основными **задачами** изучения дисциплины являются:
- Обход архитектурных ограничений.
- Небезопасное хранение данных.
- Небезопасная передача данных.
- Небезопасная аутентификация.
- Слабая криптостойкость;
- Небезопасная авторизация;
- Контроль содержимого клиентских приложений
- Модификация данных
- Анализ исходного кода
- Скрытый функционал

10. Место учебной дисциплины в структуре ООП: Дисциплина «Безопасность мобильных приложений» входит в базовую часть программы Магистратуры (М4). Изучение данного курса должно базироваться на знании обучающимися материала OWASP Mobile Security Project..

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников): ПК-1.1, ПК-5.2, ПК-5.3

Код	Название компетенции	Код(ы)	Индикаторы	Планируемые результаты обучения
ПК-5	Способен выбирать технологии и средства разработки мобильных приложений, определять ключевые сценарии для архитектуры мобильных приложений, разрабатывать новые алгоритмические, методические и технологические решения в сфере разработки мобильных приложений	ПК-5.2 ПК-5.3	Проектирует архитектуру, оценивание ПО, применяет в практической деятельности профессиональные стандарты в области информационных технологий. Имеет практический опыт в выборе технологий и средств разработки ПО, определяет цели, предположения и ограничения.	Знать: элементы архитектурных решений информационных систем, технологии и средства разработки программного обеспечения Уметь: проектировать архитектуру, оценивать ПО, применять в практической деятельности профессиональные стандарты в области информационных технологий. Владеть: выбором технологий и средств разработки ПО, определением целей, предпочтений и ограничений.
ПК-1	Способен проводить работы по обработке и анализу научно-технической информации результатов исследований	ПК-1.1	Обладает фундаментальными знаниями в области математических и естественных наук, информационно-	Знать: алгоритмы решения поставленной задачи с учетом имеющихся ресурсов Уметь: формировать основные методы и подходы к проведению научно-исследовательских работ. Владеть: методами решения прикладных задач в профессиональной сфере деятельности.

			коммуникационных технологий.	

12. Объем дисциплины в зачетных единицах/час 3 / 108.

Форма промежуточной аттестации зачет с оценкой.

13. Виды учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ 1	№ семестра	…
Аудиторные занятия		36	36		
в том числе:	лекции	12	12		
	практические				
	лабораторные	24	24		
Самостоятельная работа		72	72		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __ час.)*					
Итого:		108	108		

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Введение в безопасность мобильных приложений	История формирования, Ключевые области в обеспечении безопасности мобильных приложений, хранение данных, общение с сервером, авторизация и аутентификация, взаимодействие с ОС, качество кода и эксплойты, типы тестирования.	https://edu.vsu.ru Безопасность мобильных приложений
1.2	Обеспечение безопасности в ОС iOS	Песочница приложения, раздел пользователя, Secure Enclave, Модуль шифрования, Корневой сертификат, безопасная последовательность загрузки, TouchId, FaceId, Шифрование и защита данных, иерархия ключей, код-пароли, классы защиты данных, защита данных связки ключей	https://edu.vsu.ru Безопасность мобильных приложений
1.3	Обеспечение безопасности в ОС Android	Библиотеки криптографии, Биометрия, Шифрование и защита дынных, корневой сертификат, root доступ, лаунчеры, сертификация устройств, открытость ядра ОС, код-пароли, защита паролей.	https://edu.vsu.ru Безопасность мобильных приложений
1.4	Тестирование безопасности мобильных приложений	Тестирование белого ящика, тестирование четного ящика, тестирование серого ящика, симуляция атак «человек посередине», доступ к зашифрованным данным на диске, устройства с root/jailbreak, статический анализ кода, динамический анализ кода	https://edu.vsu.ru Безопасность мобильных приложений
1.5	Основные типы атак и эксплойтов	Sql инъекции, прямые ссылки, браузер в приложении, обратный инжиниринг	https://edu.vsu.ru Безопасность мобильных приложений
1.6	Авторизация и аутентификация	Подходы для обеспечения авторизации и аутентификации, основные уязвимости и атаки, хранение ключей и сессий.	https://edu.vsu.ru Безопасность мобильных приложений
1.7	Общение с сервером	Основные атаки на публичном wi-fi, Протоколы HTTP, HTTPS, SSL, TLS, VPN	https://edu.vsu.ru Безопасность мобильных приложений

1.8	Взаимодействие с ОС	Генерация случайных последовательностей, peer-to-peer соединения, локальное хранение данных, использование встроенных инструментов для аутентификации и авторизации пользователя, использование сторонних OAUTH 2.0 сервисов, взаимодействие с аппаратным комплексом ОС, реверс-инжиниринг	https://edu.vsu.ru Безопасность мобильных приложений
2. Практические занятия			
2.1	Тестирование общения с сервером.	Тестирование публичного приложение на обеспечение безопасного соединения с сервером-атака «человек-посередине».	https://edu.vsu.ru Безопасность мобильных приложений
2.2	Алгоритмы шифрования AES	Изучение принципов работы AES алгоритмов шифрования	https://edu.vsu.ru Безопасность мобильных приложений
2.3	Алгоритмы TLS	Разработка последовательности для стандарты TLS соединения	https://edu.vsu.ru Безопасность мобильных приложений
2.4	Авторизация	Авторизация, основные подходы и принципы	https://edu.vsu.ru Безопасность мобильных приложений
2.5	Аутентификация	Аутентификация, основные подходы и принципы	https://edu.vsu.ru Безопасность мобильных приложений
2.6	OAUTH 2.0	OAUTH 2.0 – обработка и хранение токенов сессии.	https://edu.vsu.ru Безопасность мобильных приложений
2.7	Биометрия	Использование Биометрии для аутентификации и авторизации пользователя	https://edu.vsu.ru Безопасность мобильных приложений
2.8	Обеспечение полного комплекса защиты клиент-серверного взаимодействия	Использование SSL Pinnig, биометрии и OAUTH 2.0 для обеспечения полного комплекса защиты клиент-серверного приложения	https://edu.vsu.ru Безопасность мобильных приложений
3. Лабораторные работы			
3.1	Знакомство с Charlies	Изучение программы Charles Proxy для обеспечения атаки «человек-посередине».	https://edu.vsu.ru Безопасность мобильных приложений
3.2	Разработка программ, содержащих алгоритм AES.	Реализация на любом ЯП полного алгоритма из семейства AES	https://edu.vsu.ru Безопасность мобильных

			приложений
3.3	Разработка программ, содержащих алгоритмы TLS.	Реализация полной последовательности TLS для безопасного соединения с сервером.	https://edu.vsu.ru Безопасность мобильных приложений
3.4	Разработка программ, содержащих авторизацию.	Разработка программы с авторизацией пользователя	https://edu.vsu.ru Безопасность мобильных приложений
3.5	Разработка программ, содержащих аутентификацию	Разработка программы с аутентификацией пользователя	https://edu.vsu.ru Безопасность мобильных приложений
3.6	Знакомство с OAUTH 2.0	Разработка программы обеспечивающей OAUTH 2.0 соединение с сервером	https://edu.vsu.ru Безопасность мобильных приложений
3.7	Биометрия	Разработка программы обеспечивающей безопасное хранение ключей при помощи биометрии	https://edu.vsu.ru Безопасность мобильных приложений
3.8	Обеспечение полного комплекса защиты клиент-серверного взаимодействия	Разработка клиент-серверного мобильного приложения, обеспечивающее полную защиту пользовательских данных.	https://edu.vsu.ru Безопасность мобильных приложений

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Введение в безопасность мобильных приложений	1		4	4	10
2	Обеспечение безопасности в ОС iOS	2		4	4	10
3	Обеспечение безопасности в ОС Android	2		4	4	10
4	Тестирование безопасности мобильных приложений	2		4	16	22
5	Основные типы атак и эксплойтов	2		4	24	30
6	Авторизация и аутентификация	2		4	12	18
7	Общение с сервером	2		4	12	18
8	Взаимодействие с ОС	1		6	18	26
	Итого:	12		24	72	108

14. Методические указания для обучающихся по освоению дисциплины
Работа с конспектами лекций, выполнение лабораторных заданий, заданий текущей и промежуточной аттестаций. При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*
а) основная литература**:**

№ п/п	Источник
1	Здзиарски, Дж. iPHONE. Разработка приложений с открытым кодом [Электронный ресурс] / Дж. Здзиарски. - 2-е изд. - СПб.: БХВ-.петербург, 2009. - 357 с. - Режим доступа: http://znanium.com/bookread2.php?book=48937
	Дарвин Ян Ф Android сборник рецептов: задачи и решения для разработчиков приложений. /Ян Ф. Дарвин. М:Вильямс, 2017.-768 с.
3	*Официальная документация по обеспечению безопасности ОС iOS: https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf*

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)***:**

№ п/п	Источник
	www.lib.vsu.ru – ЗНБ ВГУ
5	OWASP Mobile Security Project / 29 August 2019, at 08:11: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
6	Официальная документация по обеспечению безопасности ОС Android: *https://developer.android.com/training/articles/security-tips*
7	*https://edu.vsu.ru - Образовательный портал «Электронный университет ВГУ»- Электронный ресурс Безопасность мобильных приложений.*

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Для реализации учебного процесса используется бесплатная версия проксирования трафика Charles Proxy, а также бесплатные среды разработки xCode и Android Studio. Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Безопасность мобильных приложений», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.

18. Материально-техническое обеспечение дисциплины:

1. Мультимедийная лекционная аудитория (корп. 1, ауд. 9), рабочее место преподавателя Mac Pro, мультимедиа-проектор Optoma EP780, микрофон, аудиосистема. столы 15 шт.,стулья 30 шт. доступ к фондам учебно-методической документации, электронным библиотечным системам, выход в Интернет.

2. Компьютерный класс (корп. 1, ауд. 9) рабочее место преподавателя Mac Pro, мультимедиа-проектор Optoma EP780, доступ к фондам учебно-методической документации, электронным библиотечным системам, выход в Интернет.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Введение в безопасность мобильных приложений, Обеспечение безопасности в ОС iOS, Обеспечение безопасности в ОС Android,	ПК-1	ПК-1.1	КИМы (для проведения текущей и итоговой аттестации) Задания для лабораторных раб
2	Тестирование безопасности мобильных приложений, Основные типы атак и эксплойтов, Авторизация и аутентификация, Общение с сервером, Взаимодействие с ОС	ПК-1	ПК-1.1	КИМы (для проведения текущей и итоговой аттестации) Задания для лабораторных раб
3	Введение в безопасность мобильных приложений, Обеспечение безопасности в ОС iOS,	ПК-5	ПК-5.2	КИМы (для проведения текущей и итоговой аттестации) Задания для лабораторных работ
4	Обеспечение безопасности в ОС Android, Тестирование безопасности мобильных приложений, Основные типы атак и эксплойтов, Авторизация и аутентификация, Общение с сервером, Взаимодействие с ОС	ПК-5	ПК-5.3	КИМы (для проведения текущей и итоговой аттестации) Задания для лабораторных работ

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: Лабораторная работа

Примеры лабораторных работ

1. Дано приложение, проведите его полное тестирование обеспечения безопасности клиент-серверного взаимодействия и безопасности хранения пользовательских данных, сформируйте отчет о найденных уязвимостях и встроенных защитах.

2. Реализуйте алгоритм шифрования из семейства AES, объясните в чем заключается сложность взлома этого алгоритма, какие пути атаки могут быть предприняты.

3. Реализуйте мобильное приложение совершающее безопасную авторизацию пользователя.

4. Реализуйте мобильное приложение совершающее безопасную аутентификацию пользователя.

5. Реализуйте клиент-серверное мобильное приложение, обеспечивающее полную защиту пользовательских данных.

Описание технологии проведения

Зачет с оценкой проходит в письменной форме

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса; защиты лабораторных работ, выполнения контрольных работ.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования. Промежуточная аттестация по итогам освоения дисциплины проводится в форме зачета с оценкой и экзамена. Для получения положительной итоговой оценки необходимо выполнение всех лабораторных и контрольных работ.

При оценивании используется следующая шкала:

5 баллов ставится, если обучающийся демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно оперирует приобретенными знаниями, умениями, применяет их при решении практических задач;

4 балла ставится, если обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач;

3 балла ставится, если обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач;

2 балла ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям.